UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,494	09/21/2004	Terry M. Olkin	60468.300801	5493

32112 7590 09/17/2007

INTELLECTUAL PROPERTY LAW OFFICES
1901 S. BASCOM AVENUE, SUITE 660
CAMPBELL, CA 95008

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
09/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/711,494	OLKIN ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. At present, the pending claims are 1 – 34.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, 13 and 24 (& dependent claims) as being unpatentable over claims 1, 11 and 20 (& dependent claims) of U.S. Patent Copending Application No 10/711,495 due to obviousness-type provisional double patenting, Applicant disagrees the rejections with the following assertions:

- (a) Applicant asserts that the instant application recites claims to "determine whether an email comes from a purported originator (i.e. authentication of the source of an email)", whereas "authentication of a email" as stated in the Office action would mean to authenticate the content of a e-mail. Examiner notes "authentication of a email" does not necessarily exclude the authentication of either the source or the content of email since the email content would not be trustable if the source is un-trusted (i.e. they are closely related in security).

- (b) Applicant asserts that the present claims do not recite URL links and they do not recite elements to deliver e-mails. The present claims recite code segments, apparatus, and steps to process e-mails, regardless of how they are delivered. Examiner notes “a desired email delivery” assures “a successful email process”. As mentioned in response to argument (a), "authentication of a email" does not necessarily exclude the authentication of either the source or the content of email; on this regard, the

claims of the instant application recites "the email includes an authenticity mark including an originator identifier and encrypted data and determine whether said encrypted data decrypts successfully with information based on said authenticity mark and said decrypted data"; while the claims of the co-pending application recites "extracting an originator identifier and encrypted data from the hyperlink (i.e. URL link) and determining whether the hyperlink includes said originator identifier and said encrypted data decrypts successfully". Therefore, considering the use of a URL link to deliver an email as well-known in the field at the time the invention was made – for example, a well-known content bearing WebDAV is a technology that stands for "Web Distributed Authoring and Versioning" – Examiner notes the instant application is not patentably distinct from the co-pending application.

- (c) Applicant asserts in the case of the '495 co-pending application, the claims recite code segments, apparatus and steps that (i) listen for an activation of the hyperlink and (ii) redirect to another URL. There is nothing analogous to these in the instant claims. Examiner respectfully notes a set of *narrower* claim limitations of the co-pending application is sufficiently qualified for the rejection of the *broader* claim limitations of the instant application regarding obviousness-type provisional double patenting subject matters *from the same inventor*.

4. As per claim 1, Applicant disagrees the rejections with the following assertions:

- (a) Applicant asserts that Garib does not teach "the email includes an authenticity mark including originator identifier and encrypted data". Examiner respectfully disagrees because an originator identifier can be considered as one type of identifiers that can uniquely distinct the email originator such as either the sender / source true identifier or a digital signature that can be reasonably assured the identity of the sender – in light of

that, Garib teaches "authenticity means that the recipient can be reasonably assured of the identity of the sender (i.e., that the received message was actually sent by the party who claims to be the sender), where digital signature methods, as known in the art, can be used to ensure the authenticity of a message (Garib: Column 3 Line 47 – 52)" and Garib also teaches "the message hash value is appended to the unencrypted message and is thereafter encrypted along with the message (Garib: Column 6 Line 30 – 35)" and "data encrypted with the private key can only be decrypted with public key (Garib: Column 4 Line 49 – 50)" – Examiner notes the recipient must be able to extract the sender (or source) identifier from the received email message in order to use the correct public key corresponding to the sender (or source). Therefore, Garib does teach the email includes an authenticity mark including originator identifier and encrypted data and as such Applicant's arguments are respectfully traversed.

- (b) Applicant asserts that Garib does not teach "a code segment that decrypts said encrypted data based on said originator identifier, into decrypted data". Examiner respectfully disagrees – please refer to the similar response to argument (a) that can be reasonably interpreted to meet the claim language. However, Applicant asserts "employing PKI digital signatures is impractical with e-mails in bulk and is simply impossible if recipients are not set-up beforehand. In PKI a sender always needs a recipient's public key before a message can

be sent and the present invention is not subject to these limitations (remarks: Page 4 / 6th Par)". Examiner respectfully asserts Applicant's argument has no merit since the alleged limitation has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Double Patenting

The nonstatutory provisional double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

1. Claims 1, 13 and 24 (& dependent claims 2 – 7, 9, 12, 14 – 18, 20, 23, 25 – 29, 31 and 34) are rejected under the judicially created doctrine of obviousness-type provisional double patenting as being unpatentable over claims 1, 11 and 20 (& dependent claims 2 – 4, 6, 8 – 10, 12, 13, 15, 17 – 19, 21, 23, 25 and 26) of U.S. Patent Copending Application No 10/711,495. Although the conflicting claims are not identical, they are not patentably distinct from each other because (a) the instant application is directed toward an authentication of a email and the copending application is directed toward an authentication of a URL link; however, the method of using a URL link to deliver an email is considered and recognized as obvious and well-known in the field at the time the invention was made -- for example, a well-known content bearing

WebDAV is a technology that stands for "Web Distributed Authoring and Versioning"; by using WebDAV, one just need to send the HTTP / URL link associated with the email instead of emailing the entire file (see the following Office action below: accessing an email message remotely between a client browser and an internet server), and (b) the "authenticity mark" as recited in the instant application is equivalent to the "originator identifier and encrypted data" as recited in Copending Application No 10/711,495. For further information of rejections, please refer to the section of ***Response to Argument***.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 3 – 9, 10, 13 – 20, 21, 24 – 29 – 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Garib (U.S. Patent 6,728,378).

As per claim 1, Garib teaches **a computer program, embodied on a computer readable storage medium, for assisting a user to determine whether an email comes from a purported originator** (Garib: Column 12 Line 60 – 63 and Column 16 Line 26 – 27: a claimed

source of an email message is indeed a purported originator), **the computer program comprising**:

a code segment that determines with a computerized system whether the email includes an authenticity mark including an originator identifier and encrypted data (Garib: Column 12 Line 60 – 63, Column 3 Line 47 – 52, Column 6 Line 30 – 35, Column 4 Line 49 – 50, Column 16 Line 26 – 27 and Column 7 Line 5 – 12: an originator identifier can be considered as one type of identifiers that can uniquely distinct the email originator such as either the sender / source true identifier or a digital signature that can be reasonably assured the identity of the sender – in light of that, Garib teaches "authenticity means that the recipient can be reasonably assured of the identity of the sender (i.e., that the received message was actually sent by the party who claims to be the sender), where digital signature methods, as known in the art, can be used to ensure the authenticity of a message (Garib: Column 3 Line 47 – 52)" and Garib also teaches "the message hash value is appended to the unencrypted message and is thereafter encrypted along with the message (Garib: Column 6 Line 30 – 35)" and "data encrypted with the private key can only be decrypted with public key (Garib: Column 4 Line 49 – 50)" – Examiner notes the recipient must be able to extract the sender (or source) identifier from the received email message in order to use the correct public key corresponding to the sender (or source));

a code segment that decrypts said encrypted data based on said originator identifier, into decrypted data (Garib: please refer to the similar rationale for rejection set forth as above);

a code segment that presents to the user on a display unit (Garib: Column 12 Line 65 – 66):

whether the email includes said authenticity mark (Garib: Column 16 Line 23 – 29);

whether said encrypted data decrypts successfully; and information based on said authenticity mark and said decrypted data (Garib: Column 13 Line 51 – 59: the validation result is directed to the web browser to indicate / display the problem of the message).

As per claim 13 and 24, Garib teaches a system for assisting a user to determine whether an email comes from a purported originator (Garib: Column 12 Line 60 – 63 and Column 16 Line 26 – 27: a claimed source of an email message is indeed a purported originator), the system comprising:

a computerized system having a display unit (Garib: Column 12 Line 65 – 66);

a logic in said computerized system that determines whether the email includes an authenticity mark including an originator identifier and encrypted data (Garib: Column 12 Line 60 – 63, Column 6 Line 30 – 35, Column 16 Line 26 – 27 and Column 7 Line 5 – 12: both of the claimed source (considered as an originator identifier) and the encrypted message hash value embedded on the email message are qualified to serve as an authenticity mark for validating the integrity of email message);

a logic in said computerized system that decrypts said encrypted data based on said originator identifier, into decrypted data (Garib: Column 15 Line 20 – 23: (a) a data element is encrypted at the sender by using its private key (b) the receiving entity knows the corresponding public key of the sender and (c) the receiving entity decrypts the data to ensure the validity of the received signature / encrypted hash value);

a logic in said computerized system that that presents to the user, on said display (Garib: Column 12 Line 65 – 66):

whether the email includes said authenticity mark (Garib: Column 16 Line 23 – 29);

whether said encrypted data decrypts successfully; and information based on said authenticity mark and said decrypted data (Garib: Column 13 Line 51 – 59: the validation result is directed to the web browser to indicate / display the problem of the message).

As per claim 3, 14 and 25, Garib teaches said code segment (that determines) runs as a service in said computerized system (Garib: Column 13 Line 32 – 35 and Column 12 Line 55 – 63: running as an internet HTTP web browser email account service including the authentications).

As per claim 4, 15 and 26, Garib teaches said code segment (that determines) includes a hypertext transport protocol (HTTP) server (Garib: Column 2 Line 32 – 38, Column 3 Line 4 – 15: world wide web email account access via a HTTP server and a client web browser).

As per claim 5, 16 and 27, Garib teaches said code segment (that determines) listens at a port in said computerized system for a request for hypertext markup language (HTML) content and extracts said authenticity mark from a uniform resource locator (URL) link requesting said HTML content (Garib: Column 2 Line 32 – 38: extracting email message formatted in HTML that includes a authenticity mark and can be accessed from www (i.e. a URL link) – Examiner notes any www/HTTP protocol must include a IP address (either a public or a private IP address) and an associated port (either a assigned / fixed or a dynamic port)).

As per claim 6, 17 and 28, Garib teaches said code segment (that presents) further presents information to the user based on said originator identifier (Garib: Column 15 Line 20 – 23: the receiving entity uses the public key corresponding to the sender (i.e. originator identifier) to decrypt the data and presents the decrypted information to the user).

As per claim 7, 18 and 29, Garib teaches a code segment that matches said originator identifier to one of a plurality of registered originators maintained in a storage unit, to retrieve a decryption key associated with said originator identifier for use by said code segment that decrypts (Garib: Column 15 Line 20 – 23 / Line 39 – 41 and Column 16 Line 25 – 26: the receiving entity decrypts the email message and checks the received hash value by using the public key from stored memory to validate the claimed source).

As per claim 8, 19 and 30, Garib teaches said code segment (that determines) compares a checksum from said authenticity mark against contents of the email; and said code segment (that presents) further presents to the user information based on said checksum (Garib: Column 6 Line 30 – 35 and Column 13 Line 51 – 59: a hash / checksum value is generated the entire email content).

As per claim 9, 20 and 31, Garib teaches said code segment (that decrypts) employs a public key of said purported originator (Garib: Column 15 Line 20 – 23 / Line 39 – 41 and Column 16 Line 25 – 26: the receiving entity decrypts the email message and checks the received hash value by using the public key from stored memory to validate the claimed source).

As per claim 10, 21 and 32, Garib teaches said code segment (that decrypts) extracts at least one of a timestamp, a topic, and a user identifier from said encrypted data; and said code segment that presents further presents to the user information based on at least one of said timestamp, said topic, and said user identifier (Garib: Column 12 Line 55 – 59, Column 13 Line

51 – 59: the decrypted email message that must include a sender identifier / topic is directed to the web browser for display).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Garib (U.S. Patent 6,728,378), and in view of Dunnion et al. (U.S. Patent 2002/0199119).

As per claim 2, Garib does not disclose expressly the computer program is digitally signed.

Dunnion teaches the computer program is digitally signed (Dunnion: Para [0099]: the entire downloaded program can be digitally signed for security reason to ensure that the software downloaded is actually that provided by the supplier and has not been replaced or altered).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Dunnion within the system of Garib because (a) Garib teaches encrypting / decrypting an email message and to authenticate the requesting user with a signed data signature / hash value (Garib: Column 12 Line 60 – 63, Column 16 Line 26 – 27 and Column 7 Line 5 – 12), and (b) Dunnion teaches providing a method of a security

services system where not only the data files and email traffic need to be secured but also the entire downloaded program can be digitally signed for security reason to ensure that the software downloaded is actually that provided by the supplier and has not been replaced or altered (Dunnion: Para [0005] and Para [0099]).

4. Claims 11, 22 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garib (U.S. Patent 6,728,378), in view of Connery (U.S. Patent 6,606,709).

As per claim 11, 22 and 33, Garib does not disclose a code segment that compares said timestamp to preset timeliness criteria; and wherein said code segment that presents emphasizes said information based on said timestamp when said timeliness criteria are deviated from.

Connery teaches a code segment that compares said timestamp to preset timeliness criteria; and wherein said code segment that presents emphasizes said information based on said timestamp when said timeliness criteria are deviated from (Connery: Column 8 Line 16 – 22: a timestamp test in a remote management system by using a timestamp field that carries the time when the management system sent message and the end system checks the timestamp to determine whether it is within a pre-specified time window D seconds in width, i.e., current time - 0.5 * D <= timestamp <= current time + 0.5 * D).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Connery within the system of Garib because (a) Garib teaches accessing an email message remotely between a client browser and an internet server; and encrypting / decrypting an email message and further authenticate the requesting user with a signed data signature / hash value (Garib: Column 12 Line 60 – 63, Column 16 Line

26 – 27 and Column 7 Line 5 – 12), and (b) Connery teaches providing an enhanced security mechanism in a remote management system by using a timestamp test that includes a timestamp field carrying the time when the management system sent message and the end system checks the timestamp to determine whether it is within a pre-specified time window (Connery: Column 8 Line 16 – 22).

5. Claims 12, 23 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garib (U.S. Patent 6,728,378), and in view of Haitsuka et al. (U.S. Patent 6,766,369).

As per claim 12, 23 and 34, Garib does not disclose said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

Haitsuka teaches said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window (Haitsuka: Column 7 Line 35 – 37, Column 8 Line 44 – 47 and Column 10 Line 49 – 52: the display can have not only a browser window but also a client window; where the client window is generated / controlled by the local client application).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Haitsuka within the system of Garib because (a) Garib teaches accessing an email message remotely between a client browser and an internet server; and encrypting / decrypting an email message and further authenticate the requesting user with a signed data signature / hash value (Garib: Column 12 Line 60 – 63, Column 16 Line 26 – 27 and Column 7 Line 5 – 12), and (b) Haitsuka teaches providing a flexible mechanism with a display having not only a browser window but also a client window; where the client

window is generated / controlled by the local client application during an internet SSL communication session to indicate the connection status (including the authentication for a typical SSL connection) for the clarity purpose to avoid being confused with the display of browser window (Connery: Column 7 Line 35 – 37 and Column 10 Line 49 – 52 / Line 43 – 45).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100